Building HAProxy so that it can use TLSv1.3

This page gives an outline of how to build HAProxy with OpenSSL so it can use TLS v1.3. It assumes Ubuntu 16.04 as the platform.

Build Openssl

In order to have TLS 1.3 support you will need to grab version 1.1.1 of OpenSSL.

These instructions build OpenSSL into a directory `/opt/openssl-1.1.1` to ensure that it's separate to any other OpenSSL installs on the machine.

Build OpenSSL

```
wget https://www.openssl.org/source/openssl-1.1.1.tar.gz
tar -xzf openssl-1.1.1.tar.gz
cd openssl-1.1.1
./config --prefix=/opt/openssl-1.1.1 shared
make
sudo make install
```

Build HAProxy

You need HAProxy 1.8.1 or later to enable TLS 1.3 support. We are using 1.8.13.

Build haproxy

```
sudo apt install build-essential libpcre2-dev zlib1g-dev


wget https://www.haproxy.org/download/1.8/src/haproxy-1.8.13.tar.gz
tar -xzf haproxy-1.8.13.tar.gz
cd haproxy-1.8.13/
make TARGET=linux2628 CPU=native USE_PCRE2=1 USE_PCRE2_JIT=1 USE_OPENSSL=1 SSL_LIB=/opt/openssl-1.1.1/lib
SSL_INC=/opt/openssl-1.1.1/include USE_ZLIB=1
sudo make install


# Edit the haproxy.service unit file and ensure you have
[Service]
Environment=LD_LIBRARY_PATH=/opt/openssl-1.1.1/lib/
```

Modify the HAProxy configuration

Add the following to the HAProxy config (Note the *ssl-default-bind-ciphers* and *ssl-default-bind-options* lines), updating any paths as required.

If you only want TLSv1.3 with no fallback to TLSv1.2 then set *ssl-default-bind-options* to *force-tlsv13*

```
global
        log /dev/log    local0
        chroot /usr/local/var/lib/haproxy
        user haproxy
        group haproxy
        maxconn  4000
        pidfile  /usr/local/var/run/haproxy.pid
        tune.ssl.default-dh-param  2048
        ssl-default-bind-ciphers TLS13-AES-256-GCM-SHA384:TLS13-AES-128-GCM-SHA256:TLS13-CHACHA20-POLY1305-
SHA256:EECDH+AESGCM:EECDH+CHACHA20
        ssl-default-bind-options no-sslv3 no-tlsv10 no-tlsv11

        # Default SSL material locations
        ca-base /etc/ssl/certs
        crt-base /etc/ssl/private

defaults
        balance roundrobin
        timeout  http-request 10s
        timeout  queue 1m
        timeout  connect 10s
        timeout  client 1m
        timeout  server 1m
        timeout  check 10s

listen dns
        bind :::853 v4v6 tfo ssl crt /etc/certs/keycert.pem
        mode tcp
        server server1 127.0.0.1:9999
```

Note the keycert.pem file is the concatenation of the certificate chain and key into one file which is what HAProxy requires.

Create required paths

The above configuration sets HAProxy to run chroot in a directory `/usr/local/var/lib/haproxy`. It's necessary to create this directory. OpenSSL also needs access to `/dev/urandom` and `/dev/random` in the chroot.

```
# mkdir -p /usr/local/var/lib/haproxy/dev
# cd /usr/local/var/lib/haproxy/dev
# mknod urandom c 1 9
# mknod random c 1 8
```